(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 436 518 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
18.12.1996 Bulletin 1996/51

(51) Int Cl.[6]: **H04Q 7/20**, H04M 1/72

(21) Application number: **91300092.3**

(22) Date of filing: **07.01.1991**

(54) Radiotelephone controller configured for coresident secure and nonsecure modes

Funktelefon-Steuerung mit einer geschützten als auch einer ungeschützten Arbeitsweise

Controleur de radiotéléphone configuré pour un fonctionnement en mode protégé et non protégé

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB IT LI LU NL SE

(30) Priority: **05.01.1990 US 461570**

(43) Date of publication of application:
10.07.1991 Bulletin 1991/28

(73) Proprietor: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Muellner, Grazyna E.**
  Bartlett, Illinois 60103 (US)
- **Pini, Rafele**
  Norridge, Illinois 60656 (US)
- **Cashen, Dennis**
  Lake Zurich, Illinois 60047 (US)
- **Marry, Patrick J.**
  Cary, Illinois 60013 (US)
- **Ford, David K.**
  Mesa, Arizona 85203 (US)

(74) Representative: **Dunlop, Hugh Christopher et al**
Motorola,
European Intellectual Property,
Midpoint,
Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(56) References cited:
EP-A- 0 301 740
EP-A- 0 308 219
WO-A-91/09484
DE-A- 3 420 874

EP 0 436 518 B1

Description

Background of the Invention

The present invention is generally related to a controller for a radiotelephone, and more particularly to a radiotelephone microcontroller having a secure mode of operation and a nonsecure mode of operation, each mode sharing common portions of a microcontroller while retaining independent secure and nonsecure functions.

Previously, operation in two separate and functionally distinct modes - providing secure operation for one application and nonsecure operation for another - has been accomplished using several microcontrollers. Each microcontroller would operate in a wholly independent fashion, employing separate hardware while operating simultaneously beginning at power up. As a particular example, a mobile radiotelephone system such as that employed in the Nordic countries (and generally known as the Nordic Mobile Telephone, or NMT) and implementing SIS (Subscriber Identity Security - which is further defined in SIS Addendum to NMT DOC 900-3, dated July 1, 1988) has required three microcontrollers. The first microcontroller, the main system microcontroller, has been responsible for the radiotelephone system process execution. The second microcontroller, the display microcontroller, has been responsible for both display and keypad functions and interface with the radiotelephone user. The third microcontroller, the SIS microcontroller, has been responsible for the security of the SAK (Subscriber Authentication Key, the telephone call authorization number which is further described in SIS Addendum to NMT DOC 900-3 dated July 1, 1988 and as defined by each of the Nordic countries) and intermediate calculations required in the use of the SAK. The SAK itself is a random and user-specific 120 bit binary word which, among other parameters, is programmed into the radiotelephone unit at the point at which the user takes possession of the radiotelephone equipment. It is used when a radiotelephone call is to be made to ensure that the radiotelephone equipment is authorized to make a call. Typically, the SAK is not used in receiving a call.

In miniature portable radiotelephones (such as the MICROTAC portable radiotelephone available from Motorola, Inc. as model number F09EFD6930AA) physical space is at a premium and techniques of reducing the size of the electronic circuitry are required to achieve the necessary size reductions. Merely increasing the processing capacity of one microcontroller and loading both the nonsecure and the secure operating modes into the one microcontroller does not protect the secure operation mode from undesired external access. Furthermore, since the secure operation mode includes not only the storage and handling of the SAK but also the calculations and intermediate results from the calculation, both the storage and the calculations must be protected from access.

In EP-A-0 308 219, there is disclosed a microcomputer which is operable either in an internal program mode, wherein the microcomputer functions in accordance with an internally stored program, or in an external program mode wherein the microcomputer functions in accordance with a program stored in a memory external to the microcomputer, whereby internal RAM security is provided during the external program mode.

In EP-A-0 301 740 there is disclosed a radiotelephone having a processor controlling its operation and a card reader for reading user identification data from a card. The identification data of the card of the user authorised to use the radiotelephone are stored in non-erasable memory of the processor , whereupon the radiotelephone operates in a mode such that it can only be used with this particular card.

Summary of the Invention

Accordingly, the invention provides a radiotelephone apparatus which communicates with a fixed site, the radiotelephone including a controller having an internal secure mode of operation and internal non-secure mode of operation, the radiotelephone apparatus including a receiver for receiving a message from the fixed site, the controller responsive to said message for calculating a signed response from a stored numerical subscriber authentication key, such that said numerical subscriber authentication key and said calculations can not be accessed external to the controller, characterized in that: the controller is coupled to a serial bus having a receive line and a transmit line, a second bus, a display bus, and a keypad bus; wherein the controller comprises:

means for disabling reception of signals from the receive line, enabling transmission of signals on the transmission line, and enabling controller calculation of the signed response, in the internal secure mode;

means for enabling the transmission line, disabling the receive line, and disabling controller calculation, in the internal non-secure mode; and

means for communicating with the second bus, the display bus and the keypad bus in the internal non-secure mode.

Brief Description of the Drawings

Figure 1 is a block diagram of a radiotelephone system which may employ the present invention.

Figure 2 is a block diagram of a controller for the radiotelephone of Fig. 1 which may employ the present invention.

Figue 3 is a flowchart of the process employed by the radiotelephone of Fig. 1 to realize the present invention.

Detailed Description of the Preferred Embodiment

A portable radiotelephone 100 adapted to be used in a radiotelephone system such as the Nordic Mobile Telephone (NMT) system is shown in Figure 1. This portable radiotelephone 100 comprises a conventional radiotelephone transmitter 101 and receiver 103 to provide radio communications. The radiotelephone transmitter 101 and receiver 103 are controlled by a controller 105 which further uses a Subscriber Authentication Key (SAK) to authorize radiotelephone calls from the portable radiotelephone 100 to the wireline network via a Mobile Telephone eXchange (MTX) 107 and a fixed station 109. The user interfaces with the portable radiotelephone 100 via a conventional telephone-type matrix keypad 111 and an alphanumeric character display 113. User-generated acoustic energy is converted to an electrical signal by microphone 115 and coupled to transmitter 101 for modulation upon a radio frequency carrier and transmission from an antenna 117. Radio frequency signals received on antenna 117 from the fixed station 109 are converted to an electrical signal by receiver 103 and coupled to speaker 119 for conversion to acoustic energy for the user to hear.

Referring now to Fig. 2, a more detailed block diagram of controller 105 may be seen. A shared mode microcontroller 201, herein referred to as the SIS/Display Controller (SDC), functions in a nonsecure mode to communicate with and control the keypad 111 and the display 113, and functions in a secure mode to use the SAK. In the preferred embodiment, the SDC is a 68HC11E9 microcontroller available from Motorola, Inc. The controller accomplishes the support of both the Subscriber Identity Security (SIS) and the display/keypad functions by command interrupt switching between the two different and functionally distinct modes. Upon power-up and under standard operation the SDC 201 operates in Display Mode until an SIS calculation is requested. Upon receiving this request, the SDC 201 exits the nonsecure Display Mode and enters the secure SIS Mode. In the preferred embodiment, the SIS Mode is requested when the user wishes to make a radiotelephone call. Upon the user's request to make a call, the portable radiotelephone 100, conventionally under the control of main microcontroller 203 and the controlling program stored in memory 205, commences a radio transmission of the request to the fixed station 109 and the MTX 107. The MTX 107 and the fixed station 109 generate a random number and transmit the random number to the portable radiotelephone 100. (In the preferred embodiment, the main microcontroller is a 68HC11A8, available from Motorola, Inc.) The receiver 103 demodulates the transmission and presents the random number to the main microcontroller 203. The main microcontroller, in turn, presents the random number to the SDC 201 which calculates a signed response (SRES) from both the random number and the SAK. The SRES is transmitted back to the fixed station 109 and MTX 107 via the main microcontroller 203 and transmitter 101. If the SRES matches the independently calculated SRES of the MTX, a call is allowed; if the SRES does not match the call is terminated. Upon completion of the calculation of SRES by SDC 201, the SDC 201 exits the SIS Mode and returns to the Display Mode.

In the preferred embodiment, in order to maintain both the SRES calculating algorithm and the SAK secret, both the object code and the SAK are programmed into internal EEPROM of the SDC 201. All calculations are performed in the SDC 201 in "single chip" mode where access to the memory is limited to onboard functions and any intermediate results are stored in internal RAM. Only information which is sent back to the fixed station 109 and MTX 107 is sent to the main microcontroller 203 via the SIS bus. (Even though the chip operates in "single chip" mode, it is possible to read internal EEPROM by putting the chip into bootstrap mode. To prevent this, the configuration register's conventional NOSEC bit is set, forcing the internal EEPROM to be erased whenever bootstrap mode is entered. Since the SAK is stored, inter alia, in internal EEPROM, this feature ensures its security).

The SIS Mode and the Display Mode use separate busses to communicate with the attached devices. The SIS bus 207 couples between the SDC 201 and the main microcontroller 203 and is composed of two serial lines:
transmit (SCI txd) and receive (SCI rxd). The Display Mode uses three busses: (1) a three wire bus 209 employing a bidirectional self-clocking configuration such as described in U.S. Patent No. 4,369,516 for communication with the main microcontroller 203; (2) Port "C" bus 211, employing seven lines for communication with the ten digit LCD (Liquid Crystal Display) dot matrix display 113; and (3) the combined Port "E" and Port "B" as bus 213 for monitoring the keypad by row and column.

The process employed by SDC 201 in realizing the present invention is shown in the flowchart of Fig. 3. Commencing at the interrupt table 301, at power-up the Display Mode executive process is initialized at 303 and the Display Mode executive (main program) continues to run in the nonsecure mode. Standard control of messages written into the display 113 or of detection and decoding of keypad 111 key presses are serviced by service display request block 307. Communications with main microcontroller 203 via bus 209 are maintained by the process of block 309. Power shut down may be detected by the process of block 311 which, in the preferred embodiment, detects the depression of a power-off button. Return from each of the three nonsecure processes is to the Display Mode executive at 305.

Upon detection of a request for service via the SIS bus 207, the process leaves the Display Mode and starts the SIS executive at 315. In the preferred embodiment, the display 113 is frozen and keypad 111 is ignored during the SIS executive and subsequent processes. Reception of additional messages from the SCI rxd bus line

is disabled and the SCI txd line is enabled at 317 and the particular request from the SIS bus 207 is decoded from among six types of requests at 319. If the request is garbled or nonsensical the no task process at 321 is followed and the request is ignored. If the random number sent by the MTX 107 and the fixed station 109 has been received and conveyed by the main microcontroller 203 via SIS bus 207 the SRES is calculated from the random number and the SAK and returned via the SCI txd line of SIS bus 207, at 323. If the SAK is initially being stored in the portable radiotelephone 100, the process of accepting, storing, and verifying the SAK and the Sim (the manufacturer's reference number) is accomplished at 325 in accordance with "Specification for NMT-SIS Key Management for NMT-900", dated July 1, 1988. In the preferred embodiment, a second SAK, publically known, is used for test purposes. A test mode, at 327, may be entered via SIS bus 207 command in which the public SAK is used for test radiotelephone calls. Upon power-up, a test is made, at 329, in response to a SIS bus 207 command to check for proper operation of the SIS system and whether a SAK has been stored in the EEPROM of SDC 201. Also, a request via SIS bus 207 for the manufacturer's reference number (Sim) causes the Sim to be recalled from the EEPROM of SDC 201 and sent to the display 113. At the conclusion of the requested one of the six tasks, the SCI txd line interrupt is disabled and the SCI rxd line is enabled of SIS bus 207 at 333 and operation returns to the nonsecure Display Mode at 335.

Thus, a controller for a portable radiotelephone having the capability of operation in both a secure mode and a nonsecure mode of operation has been shown and described. The nonsecure mode and secure mode are both resident in a single microcontroller which runs the nonsecure operations until a requirement for the secure operation is requested. The nonsecure mode is disabled during the period of time the secure mode is operational and is reenabled upon completion of the secure mode operation. The secure mode cannot be accessed externally to the microcontroller. While a particular embodiment of the invention has been shown and described, it is to be understood that the invention is not to be taken as limited to the specific embodiment herein,

Claims

1. A radiotelephone apparatus (100) for communicating with a fixed site (109), the radiotelephone including a controller (105 or 201) having an internal secure mode of operation and internal non-secure mode of operation, the radiotelephone apparatus including a receiver (103) for receiving a message from the fixed site, the controller responsive to said message for calculating a signed response from a stored numerical subscriber authentication key, such that said numerical subscriber authentication key and said calculations can not be accessed external to the controller, characterized in that:

   the controller is coupled to a serial bus (207) having a receive line and a transmit line, a second bus (209), a display bus (211), and a keypad bus (213);
   wherein the controller comprises:

   means for disabling reception of signals from the receive line, enabling transmission of signals on the transmission line (317), and enabling controller calculation of the signed response, in the internal secure mode;
   means for enabling the transmission line, disabling the receive line (333), and disabling controller calculation, in the internal non-secure mode; and
   means for communicating with the second bus (209), the display bus and the keypad bus in the internal non-secure mode.

2. The radiotelephone as defined in claim 1, further including a second controller coupled to the serial bus, the second bus, and the receiver.

3. The radiotelephone as defined in claim 2, further including a keypad (111) and a display (113), wherein the display and keypad are disabled in the internal secure mode and enabled in the internal non-secure mode.

4. The radiotelephone as defined in claim 3, wherein the second bus comprises a three-wire bus with a bi-directional self-clocking configuration.

Patentansprüche

1. Funktelefongerät (100), das mit einer Feststation (109) kommuniziert, wobei das Funktelefon einen Kontroller (105 oder 201) mit einer internen gesicherten Betriebsart und einer internen ungesicherten Betriebsart umfaßt, wobei das Funktelefongerät einen Empfänger (103) zum Empfangen einer Nachricht von der Feststation umfaßt, der Kontroller auf die Nachricht anspricht, um eine bezeichnete Antwort aus einem gespeicherten numerischen Teilnehmer-Beglaubigungsschlüssel zu berechnen, so daß auf den numerischen Teilnehmer-Beglaubigungsschlüssel und die Berechnungen nicht außerhalb des Kontrollers zugegriffen werden kann, dadurch gekennzeichnet daß:

   der Kontroller mit einem seriellen Bus (207) mit einer Empfangsleitung und einer Sendeleitung, einem zweiten Bus (209), einem Anzeigebus

(211) und einem Tastaturbus (213) verbunden ist,

wobei der Kontroller umfaßt:

eine Einrichtung, die in der internen gesicherten Betriebsart den Empfang von Signalen von der Empfangsleitung sperrt, das Senden von Signalen auf der Sendeleitung (317) freigibt und die Kontrollerberechnung der bezeichneten Antwort freigibt;

eine Einrichtung, die in der internen ungesicherten Betriebsart die Sendeleitung freigibt, die Empfangsleitung (333) sperrt und die Kontrollerberechnung sperrt, und

eine Einrichtung, um in der internen ungesicherten Betriebsart mit dem zweiten Bus (209), dem Anzeigebus und dem Tastaturbus zu kommunizieren.

2. Funktelefon nach Anspruch 1, das weiter einen zweiten Kontroller umfaßt, der mit dem seriellen Bus, dem zweiten Bus und dem Empfänger verbunden ist.

3. Funktelefon nach Anspruch 2, das weiter eine Tastatur (111) und eine Anzeige (113) umfaßt, wobei die Anzeige und die Tastatur in der internen gesicherten Betriebsart gesperrt und in der internen ungesicherten Betriebsart freigegeben werden.

4. Funktelefon nach Anspruch 3, bei dem der zweite Bus einen Dreidrahtbus mit einer bidirektionalen selbsttaktenden Konfiguration umfaßt.

Revendications

1. Appareil raiotéléphonique (100) permettant de communiquer avec un site fixe (109), le radiotéléphone comportant un contrôleur (105 ou 201) ayant un mode de fonctionnement sûr interne et un mode de fonctionnement non sûr interne, l'appareil radiotéléphonique comportant un récepteur (103) permettant de recevoir un message du site fixe, le contrôleur réagissant audit message pour calculer une réponse signée à partir d'une clé d'authentification de l'abonné numérique mémorisée, de sorte qu'on ne puisse accéder ni à ladite clé d'authentification de l'abonné numérique ni auxdits calculs depuis l'extérieur du contrôleur, caractérisé en ce que :

le contrôleur est couplé à un bus série (207) ayant une ligne de réception et une ligne de transmission, un deuxième bus (209), un bus d'affichage (211) et un bus d'introduction par clavier (213) ;
dans lequel le contrôleur comprend :
un moyen permettant d'invalider la réception de signaux provenant de la ligne de réception, de valider la transmission de signaux sur la ligne de transmission (317) et de valider le calcul, par le contrôleur, de la réponse signée, en mode sûr interne ;
un moyen permettant de valider la ligne de transmission, d'invalider la ligne de réception (333) et d'invalider le calcul effectué par le contrôleur, en mode non sûr interne ;
un moyen permettant de communiquer avec le deuxième bus (209), le bus d'affichage et le bus d'introduction par clavier en mode non sûr interne.

2. Radiotéléphone selon la revendication 1, comportant en outre un deuxième contrôleur couplé au bus série, au deuxième bus, et au récepteur.

3. Radiotéléphone selon la revendication 2, comportant en outre un pavé numérique (111) et un affichage (113), dans lequel l'affichage et le pavé numérique sont invalidés en mode sûr interne et validés en mode non sûr interne.

4. Radiotéléphone selon la revendication 3, dans lequel le deuxième bus comprend un bus à trois câbles ayant une configuration d'autocadencement directionnel.

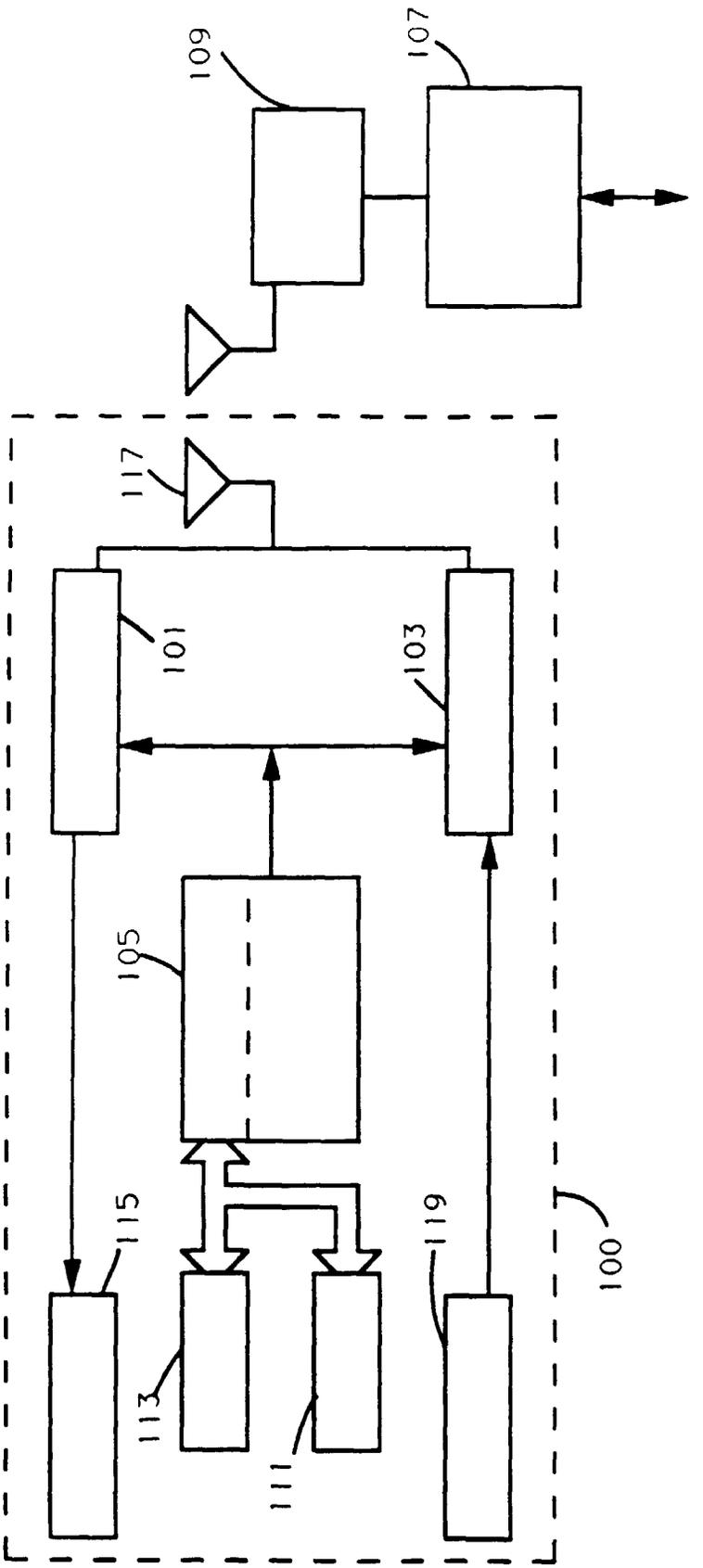

Fig. 1

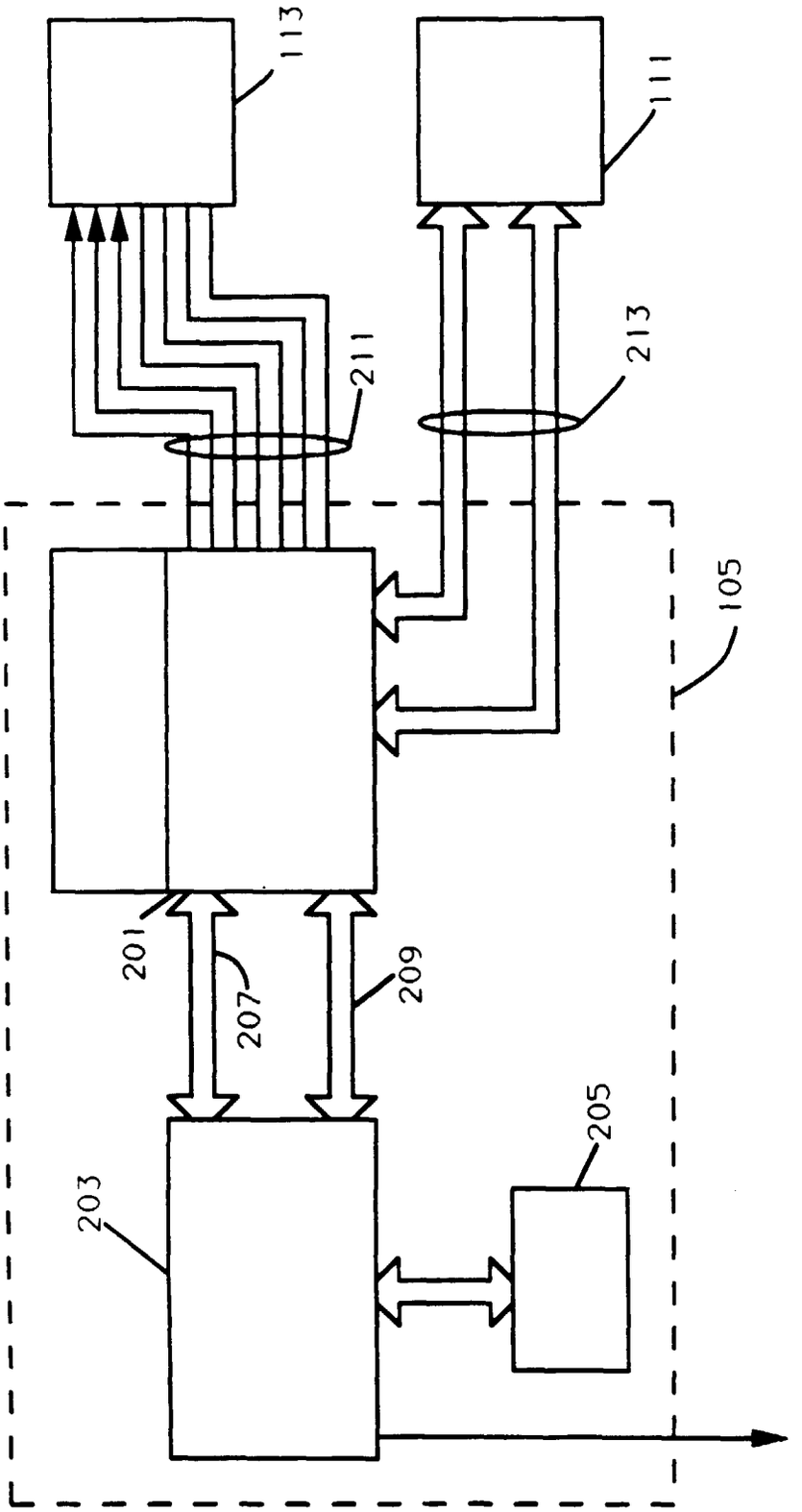

Fig. 2

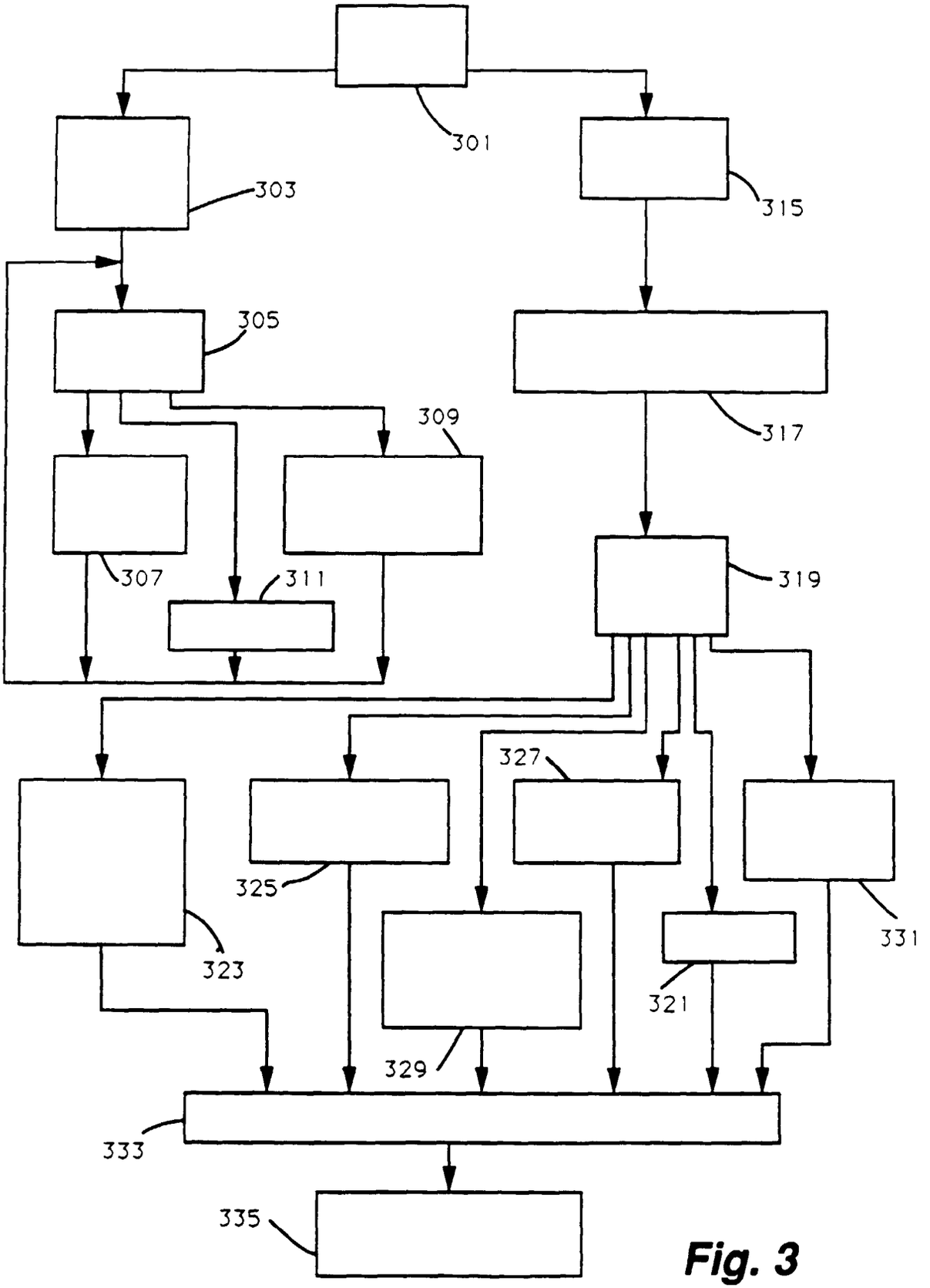
301
303
315
305
317
309
307
311
319
327
325
323
331
321
329
333
335

Fig. 3